EXHIBIT C-14
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 6 ('661 Patent)	U.S. 5,086,467 to Malek ("Malek")
A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:23-38 – "Traffic analysis is one technique employed to gather useful information from a secure communication channel without subjecting the message traffic to the rigorous cryptanalytic attack generally required to find the proper encryption key. For example, by noting the time of day during which peak traffic occurs, a cryptanalyst may derive meaningful information concerning the organizations among which communication is occurring. A sharp increase in the amount of secure traffic being transmitted among covert organizations may indicate that an important intelligence-gathering operation is about to commence. Similarly, monitoring enciphered transmissions among corporate entities may give a cryptanalyst some indication concerning imminent business transactions such as takeovers, mergers or other major financial dealings." 1:45-54 – "The improvement comprises a second signal source for providing second message signals wherein the second signal source causes the second message signals to be provided to the transmitter when the first message signals are absent. In general, these first message signals are encrypted voice messages or encrypted data signals. The second message signals, at least in part, represent dummy traffic." 2:2-6 – "In the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel." 2:38-48 – "In order to control the application of dummy traffic signals to the repeater's transmitter, as well as monitor the activity of the other signals that occur within the repeater, such as console audio and receiver output, a real time clock and control module is employed. In the preferred embodiment, the real time clock and control module, the LFSR, and the random variable generators are implemented in a commercially available microprocessor such as an MC68HC11, manufactured by Motorola, Inc. Of course, implementation may also be accomplished using discrete logic." 2:64-68 – "FIG. 1 illustrates a transmitter system generally depicted by the numeral 100. The transmitter system includes a first signal source (101) and a second signal source (102), which in this case is a dummy

	traffic generator." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	2:64-3:4 – "FIG. 1 illustrates a transmitter system generally depicted by the numeral 100. The transmitter system includes a first signal source (101) and a second signal source (102), which in this case is a dummy traffic generator. The signal source that provides signals to the transmitter (104) at any given time is determined by a switch (103). The switch (103) is directly controlled by the dummy traffic generator (102) via a control line (105)." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." Figure 1.
(b) a source of unpredictable information;	1:59-66 – "The second signal source is called a dummy traffic generator. The dummy traffic generator may be part of a repeater, which is a radio transceiver that receives signals on one frequency and retransmits these signals on another. A repeater is a communication unit generally designed to improve range in an RF communication system involving portable units, mobile units and fixed units."
(c) a processor:	3:41-44 – "A dummy traffic generator module as generally depicted by the numeral 300 can be seen in more detail in FIG. 3. The dummy traffic generator includes a bit generator (301)." 4:8-29 – "The output (313) of the bit generator (301) is also provided to the input of one analog switch (318) in the form of the dummy

	traffic input (314). Other signal sources, such as encrypted voice or data, are applied to the other analog switch (319) through the input (317) dedicated to other signal sources. When the dummy traffic PTT signal from the RTC and control module is asserted, the first analog switch (318) connects the dummy traffic signal (314) to the switch output line (316) so that it may be directed to the modulator. In the event that the RTC and control module (307) detects PTT signals from other signal sources over the PTT input line (312), dummy traffic PTT (315) will be de-asserted, thus deactivating the first analog switch (318) while activating the second analog switch (319) to allow the information signal from the other signal source to be applied to the modulator. The dummy traffic generator operates at the lowest level of priority; therefore, a dummy traffic signal may be gracefully pre-empted by actual traffic from one of the other signal sources." Figure 3.
(i) connected to said input interface for receiving and cryptographically processing said quantity,	3:30-40 – "The dummy traffic generator (204) is able to monitor the output of the receiver (202) through a secondary output line (211) and the console audio through a secondary audio line (212). When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time. These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206). Control of the switch (205) is achieved by the dummy traffic generator through the switch control output (208)." Figure 1.
(ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional electricity in said microchip during said processing; and	1:23-38 – "Traffic analysis is one technique employed to gather useful information from a secure communication channel without subjecting the message traffic to the rigorous cryptanalytic attack generally required to find the proper encryption key. For example, by noting the time of day during which peak traffic occurs, a cryptanalyst may derive meaningful information concerning the organizations among which communication is occurring. A sharp increase in the amount of secure traffic being transmitted among covert organizations may indicate that an important intelligence-gathering operation is about to commence. Similarly, monitoring enciphered transmissions among corporate entities may give a cryptanalyst some indication concerning imminent business transactions such as takeovers, mergers or other major financial dealings." 2:29-34 – "This may be accomplished by using the output of the LFSR to seed random variable generators, one of which may be used to select the duration of any dummy traffic transmission, and the other of which may be used to determine the inter-transmission delay, or time

	between transmissions." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." 3:33-35 – "When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	1:44-50 – "According to the invention, an improvement is provided to a transmitter that transmits first message signals provided by a first signal source. The improvement comprises a second signal source for providing second message signals wherein the second signal source causes the second message signals to be provided to the transmitter when the first message signals are absent." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." 3:36-38 – "These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206)."

Claim 7 ('661 Patent)	**U.S. 5,086,467 to Malek**
The device of claim 6 including program logic to activate said expending during said	2:34-37 – "In order to more easily adapt dummy traffic generation to a specific traffic model, the random variable generators which produce the duration and delay values may be subject to user programmable

processing.	limits." 3:54-4:2 – "The output (313) of the bit generator (301) provides seed values for two RV (Random Variable) generators (305 and 306). These RV generators (305 and 306) operate on the pseudo-random seed values provided by the bit generator (301) by subjecting them to the constraints of user-programmable limits, in a manner to be described later. The user-programmed limits are provided to the RV generators through separate input lines (308). The first RV generator (305) provides a number corresponding to the duration of the next dummy transmission to a real time clock and control module (307) through a dedicated input line (310). A second RV generator (306) generates the inter-transmission delay, which is the amount of time between successive dummy traffic transmissions. This delay value is supplied to the real time clock and control module (307) through another input line (311)."

Claim 8 ('661 Patent)	**U.S. 5,086,467 to Malek**
The device of claim 7 including (a) program logic implementing said source of unpredictable information; and	2:34-37 – "In order to more easily adapt dummy traffic generation to a specific traffic model, the random variable generators which produce the duration and delay values may be subject to user programmable limits." 3:54-4:2 – "The output (313) of the bit generator (301) provides seed values for two RV (Random Variable) generators (305 and 306). These RV generators (305 and 306) operate on the pseudo-random seed values provided by the bit generator (301) by subjecting them to the constraints of user-programmable limits, in a manner to be described later. The user-programmed limits are provided to the RV generators through separate input lines (308). The first RV generator (305) provides a number corresponding to the duration of the next dummy transmission to a real time clock and control module (307) through a dedicated input line (310). A second RV generator (306) generates the inter-transmission delay, which is the amount of time between successive dummy traffic transmissions. This delay value is supplied to the real time clock and control module (307) through another input line (311)." 4:29-5:12 – "FIG. 4 is a flow chart of the algorithm used by an RV generator to condition the seed value provided by the LFSR. After the START state (401), several assignment operations are performed in block 402 to assign the seed value to a variable S, a user-programmed lower limit to a variable L, and a user-programmed upper limit to a

	variable U. An iteration counter I is also initialized to zero."
(b) program logic to transmit said unpredictable information to an additional power expending circuit contained in said microchip.	4:29-5:12 – "FIG. 4 is a flow chart of the algorithm used by an RV generator to condition the seed value provided by the LFSR. After the START state (401), several assignment operations are performed in block 402 to assign the seed value to a variable S, a user-programmed lower limit to a variable L, and a user-programmed upper limit to a variable U. An iteration counter I is also initialized to zero."

Claim 9 ('661 Patent)	**U.S. 5,086,467 to Malek**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:23-38 – "Traffic analysis is one technique employed to gather useful information from a secure communication channel without subjecting the message traffic to the rigorous cryptanalytic attack generally required to find the proper encryption key. For example, by noting the time of day during which peak traffic occurs, a cryptanalyst may derive meaningful information concerning the organizations among which communication is occurring. A sharp increase in the amount of secure traffic being transmitted among covert organizations may indicate that an important intelligence-gathering operation is about to commence. Similarly, monitoring enciphered transmissions among corporate entities may give a cryptanalyst some indication concerning imminent business transactions such as takeovers, mergers or other major financial dealings." 1:45-54 – "The improvement comprises a second signal source for providing second message signals wherein the second signal source causes the second message signals to be provided to the transmitter when the first message signals are absent. In general, these first message signals are encrypted voice messages or encrypted data signals. The second message signals, at least in part, represent dummy traffic." 2:2-6 – "In the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel." 2:64-68 – "FIG. 1 illustrates a transmitter system generally depicted by the numeral 100. The transmitter system includes a first signal source (101) and a second signal source (102), which in this case is a dummy traffic generator."

	3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	2:64-3:4 – "FIG. 1 illustrates a transmitter system generally depicted by the numeral 100. The transmitter system includes a first signal source (101) and a second signal source (102), which in this case is a dummy traffic generator. The signal source that provides signals to the transmitter (104) at any given time is determined by a switch (103). The switch (103) is directly controlled by the dummy traffic generator (102) via a control line (105)." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." Figure 1.
(b) a source of unpredictable information;	1:59-66 – "The second signal source is called a dummy traffic generator. The dummy traffic generator may be part of a repeater, which is a radio transceiver that receives signals on one frequency and retransmits these signals on another. A repeater is a communication unit generally designed to improve range in an RF communication system involving portable units, mobile units and fixed units."
(c) a processor:	3:41-44 – "A dummy traffic generator module as generally depicted by the numeral 300 can be seen in more detail in FIG. 3. The dummy traffic generator includes a bit generator (301)." 4:8-29 – "The output (313) of the bit generator (301) is also provided to the input of one analog switch (318) in the form of the dummy traffic input (314). Other signal sources, such as encrypted voice or data, are applied to the other analog switch (319) through the input

	(317) dedicated to other signal sources. When the dummy traffic PTT signal from the RTC and control module is asserted, the first analog switch (318) connects the dummy traffic signal (314) to the switch output line (316) so that it may be directed to the modulator. In the event that the RTC and control module (307) detects PTT signals from other signal sources over the PTT input line (312), dummy traffic PTT (315) will be de-asserted, thus deactivating the first analog switch (318) while activating the second analog switch (319) to allow the information signal from the other signal source to be applied to the modulator. The dummy traffic generator operates at the lowest level of priority; therefore, a dummy traffic signal may be gracefully pre-empted by actual traffic from one of the other signal sources." Figure 3.
(i) connected to said input interface for receiving and cryptographically processing said quantity,	3:30-40 – "The dummy traffic generator (204) is able to monitor the output of the receiver (202) through a secondary output line (211) and the console audio through a secondary audio line (212). When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time. These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206). Control of the switch (205) is achieved by the dummy traffic generator through the switch control output (208)." Figure 1.
(ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity;	1:23-38 – "Traffic analysis is one technique employed to gather useful information from a secure communication channel without subjecting the message traffic to the rigorous cryptanalytic attack generally required to find the proper encryption key. For example, by noting the time of day during which peak traffic occurs, a cryptanalyst may derive meaningful information concerning the organizations among which communication is occurring. A sharp increase in the amount of secure traffic being transmitted among covert organizations may indicate that an important intelligence-gathering operation is about to commence. Similarly, monitoring enciphered transmissions among corporate entities may give a cryptanalyst some indication concerning imminent business transactions such as takeovers, mergers or other major financial dealings." 2:29-34 – "This may be accomplished by using the output of the LFSR to seed random variable generators, one of which may be used to select the duration of any dummy traffic transmission, and the other of which may be used to determine the inter-transmission delay, or time between transmissions."

	3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." 3:33-35 – "When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof;	1:44-50 – "According to the invention, an improvement is provided to a transmitter that transmits first message signals provided by a first signal source. The improvement comprises a second signal source for providing second message signals wherein the second signal source causes the second message signals to be provided to the transmitter when the first message signals are absent." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." 3:36-38 – "These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206)."
(e) a hardware-implemented noise production subunit connected to said source of unpredictable information and configured to expend unpredictable amounts of electricity	2:20-25 – "Thus, the output signal of the LFSR will have noise-like characteristics very similar to that of encrypted information. Because of these noise-like properties, the output of the LFSR is often termed a pseudo-random sequence." 3:45-4:1 – "The bit generator (301) is comprised of a shift register (302) with a series of taps coming from individual shift register stages. For the sake of clarity, only one such tap is shown here. These taps are added together in a modulo-2 adder (303) to form a linear feedback shift register (LFSR), as is well-known in the art. The bit generator is

based on the output of said source of unpredictable information; and	also equipped with an input register (304) through which the user may enter an initial value (320) or seed value for purposes of initializing the LFSR. The output (313) of the bit generator (301) provides seed values for two RV (Random Variable) generators (305 and 306). These RV generators (305 and 306) operate on the pseudo-random seed values provided by the bit generator (301) by subjecting them to the constraints of user-programmable limits, in a manner to be described later. The user-programmed limits are provided to the RV generators through separate input lines (308). The first RV generator (305) provides a number corresponding to the duration of the next dummy transmission to a real time clock and control module (307) through a dedicated input line (310). A second RV generator (306) generates the inter-transmission delay, which is the amount of time between successive dummy traffic transmissions. This delay value is supplied to the real time clock and control module (307) through another input line (311)." Figure 3.
(f) an activation controller, which may be activated by software contained in said device, to activate and deactivate said expending of unpredictable amounts of electricity.	3:2-4 – "The switch (103) is directly controlled by the dummy traffic generator (102) via a control line (105)." 3:30-40 – "The dummy traffic generator (204) is able to monitor the output of the receiver (202) through a secondary output line (211) and the console audio through a secondary audio line (212). When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time. These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206). Control of the switch (205) is achieved by the dummy traffic generator through the switch control output (208)." 4:17-25 – "In the event that the RTC and control module (307) detects PTT signals from other signal sources over the PTT input line (312), dummy traffic PTT (315) will be de-asserted, thus deactivating the first analog switch (318) while activating the second analog switch (319) to allow the information signal from the other signal source to be applied to the modulator."

Claim 10 ('661 Patent)	**U.S. 5,086,467 to Malek**
The device of claim 9 wherein said source of unpredictable information is a	3:45-4:1 – "The bit generator (301) is comprised of a shift register (302) with a series of taps coming from individual shift register stages. For the sake of clarity, only one such tap is shown here. These taps are added together in a modulo-2 adder (303) to form a linear feedback

hardware-implemented random number generator, and wherein said noise production subunit includes a digital-to-analog converter.	shift register (LFSR), as is well-known in the art. The bit generator is also equipped with an input register (304) through which the user may enter an initial value (320) or seed value for purposes of initializing the LFSR. The output (313) of the bit generator (301) provides seed values for two RV (Random Variable) generators (305 and 306). These RV generators (305 and 306) operate on the pseudo-random seed values provided by the bit generator (301) by subjecting them to the constraints of user-programmable limits, in a manner to be described later. The user-programmed limits are provided to the RV generators through separate input lines (308). The first RV generator (305) provides a number corresponding to the duration of the next dummy transmission to a real time clock and control module (307) through a dedicated input line (310). A second RV generator (306) generates the inter-transmission delay, which is the amount of time between successive dummy traffic transmissions. This delay value is supplied to the real time clock and control module (307) through another input line (311)." Figure 3. *See also, e.g.*, English abstracts of JP10084223, JP10197610, JP62260406, and JP62082702 (describing including a digital to analog converter in a noise production subunit).

Claim 11 ('661 Patent)	**U.S. 5,086,467 to Malek**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	1:23-38 – "Traffic analysis is one technique employed to gather useful information from a secure communication channel without subjecting the message traffic to the rigorous cryptanalytic attack generally required to find the proper encryption key. For example, by noting the time of day during which peak traffic occurs, a cryptanalyst may derive meaningful information concerning the organizations among which communication is occurring. A sharp increase in the amount of secure traffic being transmitted among covert organizations may indicate that an important intelligence-gathering operation is about to commence. Similarly, monitoring enciphered transmissions among corporate entities may give a cryptanalyst some indication concerning imminent business transactions such as takeovers, mergers or other major financial dealings." 1:45-54 – "The improvement comprises a second signal source for providing second message signals wherein the second signal source causes the second message signals to be provided to the transmitter when the first message signals are absent. In general, these first message signals are encrypted voice messages or encrypted data

	signals. The second message signals, at least in part, represent dummy traffic." 2:2-6 – "In the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel." 2:64-68 – "FIG. 1 illustrates a transmitter system generally depicted by the numeral 100. The transmitter system includes a first signal source (101) and a second signal source (102), which in this case is a dummy traffic generator." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	2:64-3:4 – "FIG. 1 illustrates a transmitter system generally depicted by the numeral 100. The transmitter system includes a first signal source (101) and a second signal source (102), which in this case is a dummy traffic generator. The signal source that provides signals to the transmitter (104) at any given time is determined by a switch (103). The switch (103) is directly controlled by the dummy traffic generator (102) via a control line (105)." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." Figure 1.
(b) an input interface for receiving a	2:64-3:4 – "FIG. 1 illustrates a transmitter system generally depicted by the numeral 100. The transmitter system includes a first signal

variable amount of power, said power consumption varying measurably during said performance of said operation;	source (101) and a second signal source (102), which in this case is a dummy traffic generator. The signal source that provides signals to the transmitter (104) at any given time is determined by a switch (103). The switch (103) is directly controlled by the dummy traffic generator (102) via a control line (105)." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." Figure 1.
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	3:30-40 – "The dummy traffic generator (204) is able to monitor the output of the receiver (202) through a secondary output line (211) and the console audio through a secondary audio line (212). When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time. These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206). Control of the switch (205) is achieved by the dummy traffic generator through the switch control output (208)." Figure 1.
(d) a noise production system for introducing noise into said measurement of said power consumption.	1:59-66 – "The second signal source is called a dummy traffic generator. The dummy traffic generator may be part of a repeater, which is a radio transceiver that receives signals on one frequency and retransmits these signals on another. A repeater is a communication unit generally designed to improve range in an RF communication system involving portable units, mobile units and fixed units." 1:67-2:6 – "The dummy traffic generator is capable of monitoring signals at the output of the repeater's receiver as well as any input that may be directed to the repeater from an associated control console. In the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel." 2:20-24 – "Thus, the output signal of the LFSR will have noise-like

	characteristics very similar to that of encrypted information. Because of these noise-like properties, the output of the LFSR is often termed a pseudo-random sequence."

Claim 12 ('661 Patent)	U.S. 5,086,467 to Malek
The device of claim 11 wherein said noise production system comprises: (a) a source of randomness for generating initial noise having a random characteristic;	1:67-2:6 – "The dummy traffic generator is capable of monitoring signals at the output of the repeater's receiver as well as any input that may be directed to the repeater from an associated control console. In the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel." 2:20-24 – "Thus, the output signal of the LFSR will have noise-like characteristics very similar to that of encrypted information. Because of these noise-like properties, the output of the LFSR is often termed a pseudo-random sequence."
(b) a noise processing module for improving the random characteristic of said initial noise; and	4:29-5:12 – "FIG. 4 is a flow chart of the algorithm used by an RV generator to condition the seed value provided by the LFSR. After the START state (401), several assignment operations are performed in block 402 to assign the seed value to a variable S, a user-programmed lower limit to a variable L, and a user-programmed upper limit to a variable U. An iteration counter I is also initialized to zero."
(c) a noise production module configured to vary said power consumption based on an output of said noise processing module.	1:59-66 – "The second signal source is called a dummy traffic generator. The dummy traffic generator may be part of a repeater, which is a radio transceiver that receives signals on one frequency and retransmits these signals on another. A repeater is a communication unit generally designed to improve range in an RF communication system involving portable units, mobile units and fixed units." 3:25-29 – "The repeater system (200) is also designed so that the operator of an associated console (not shown) can direct console audio via a console audio input (203) through the switch (205), and finally to the transmitter (206)."

Claim 13 ('661 Patent)	U.S. 5,086,467 to Malek
The device of claim 12 wherein said noise production system is	1:67-2:6 – "The dummy traffic generator is capable of monitoring signals at the output of the repeater's receiver as well as any input that may be directed to the repeater from an associated control console. In

connected to said processor and is selectively operable under the control of said processor.	the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel."

Claim 23 ('661 Patent)	**U.S. 5,086,467 to Malek**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	1:23-38 – "Traffic analysis is one technique employed to gather useful information from a secure communication channel without subjecting the message traffic to the rigorous cryptanalytic attack generally required to find the proper encryption key. For example, by noting the time of day during which peak traffic occurs, a cryptanalyst may derive meaningful information concerning the organizations among which communication is occurring. A sharp increase in the amount of secure traffic being transmitted among covert organizations may indicate that an important intelligence-gathering operation is about to commence. Similarly, monitoring enciphered transmissions among corporate entities may give a cryptanalyst some indication concerning imminent business transactions such as takeovers, mergers or other major financial dealings." 1:45-54 – "The improvement comprises a second signal source for providing second message signals wherein the second signal source causes the second message signals to be provided to the transmitter when the first message signals are absent. In general, these first message signals are encrypted voice messages or encrypted data signals. The second message signals, at least in part, represent dummy traffic." 2:2-6 – "In the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel." 2:64-68 – "FIG. 1 illustrates a transmitter system generally depicted by the numeral 100. The transmitter system includes a first signal source (101) and a second signal source (102), which in this case is a dummy traffic generator." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output

	(107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume."
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	2:64-3:4 – "FIG. 1 illustrates a transmitter system generally depicted by the numeral 100. The transmitter system includes a first signal source (101) and a second signal source (102), which in this case is a dummy traffic generator. The signal source that provides signals to the transmitter (104) at any given time is determined by a switch (103). The switch (103) is directly controlled by the dummy traffic generator (102) via a control line (105)." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." Figure 1.
(b) generating unpredictable information;	2:64-3:4 – "FIG. 1 illustrates a transmitter system generally depicted by the numeral 100. The transmitter system includes a first signal source (101) and a second signal source (102), which in this case is a dummy traffic generator. The signal source that provides signals to the transmitter (104) at any given time is determined by a switch (103). The switch (103) is directly controlled by the dummy traffic generator (102) via a control line (105)." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume."

	Figure 1.
(c) cryptographically processing said quantity, including using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by selecting between:	1:23-38 – "Traffic analysis is one technique employed to gather useful information from a secure communication channel without subjecting the message traffic to the rigorous cryptanalytic attack generally required to find the proper encryption key. For example, by noting the time of day during which peak traffic occurs, a cryptanalyst may derive meaningful information concerning the organizations among which communication is occurring. A sharp increase in the amount of secure traffic being transmitted among covert organizations may indicate that an important intelligence-gathering operation is about to commence. Similarly, monitoring enciphered transmissions among corporate entities may give a cryptanalyst some indication concerning imminent business transactions such as takeovers, mergers or other major financial dealings." 2:29-34 – "This may be accomplished by using the output of the LFSR to seed random variable generators, one of which may be used to select the duration of any dummy traffic transmission, and the other of which may be used to determine the inter-transmission delay, or time between transmissions." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." 3:33-35 – "When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time."
(c)(1) performing a computation and incorporating the result of said computation in said cryptographic processing, and	1:59-66 – "The second signal source is called a dummy traffic generator. The dummy traffic generator may be part of a repeater, which is a radio transceiver that receives signals on one frequency and retransmits these signals on another. A repeater is a communication unit generally designed to improve range in an RF communication system involving portable units, mobile units and fixed units." 1:67-2:6 – "The dummy traffic generator is capable of monitoring signals at the output of the repeater's receiver as well as any input that may be directed to the repeater from an associated control console. In

	the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel." 3:30-40 – "The dummy traffic generator (204) is able to monitor the output of the receiver (202) through a secondary output line (211) and the console audio through a secondary audio line (212). When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time. These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206). Control of the switch (205) is achieved by the dummy traffic generator through the switch control output (208)."
(c)(2) performing a computation whose output is not incorporated in said cryptographic processing; and	1:59-66 – "The second signal source is called a dummy traffic generator. The dummy traffic generator may be part of a repeater, which is a radio transceiver that receives signals on one frequency and retransmits these signals on another. A repeater is a communication unit generally designed to improve range in an RF communication system involving portable units, mobile units and fixed units." 1:67-2:6 – "The dummy traffic generator is capable of monitoring signals at the output of the repeater's receiver as well as any input that may be directed to the repeater from an associated control console. In the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel." 3:30-40 – "The dummy traffic generator (204) is able to monitor the output of the receiver (202) through a secondary output line (211) and the console audio through a secondary audio line (212). When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time. These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206). Control of the switch (205) is achieved by the dummy traffic generator through the switch control output (208)."
(d) outputting said cryptographically processed quantity to a recipient thereof.	1:44-50 – "According to the invention, an improvement is provided to a transmitter that transmits first message signals provided by a first signal source. The improvement comprises a second signal source for providing second message signals wherein the second signal source causes the second message signals to be provided to the transmitter when the first message signals are absent."

	3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." 3:36-38 – "These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206)."

Claim 24 ('661 Patent)	**U.S. 5,086,467 to Malek**
The method of claim 23 where said selecting is performed in software.	1:59-66 – "The second signal source is called a dummy traffic generator. The dummy traffic generator may be part of a repeater, which is a radio transceiver that receives signals on one frequency and retransmits these signals on another. A repeater is a communication unit generally designed to improve range in an RF communication system involving portable units, mobile units and fixed units." 1:67-2:6 – "The dummy traffic generator is capable of monitoring signals at the output of the repeater's receiver as well as any input that may be directed to the repeater from an associated control console. In the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." 3:30-40 – "The dummy traffic generator (204) is able to monitor the output of the receiver (202) through a secondary output line (211) and

	the console audio through a secondary audio line (212). When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time. These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206). Control of the switch (205) is achieved by the dummy traffic generator through the switch control output (208)."

Claim 25 ('661 Patent)	**U.S. 5,086,467 to Malek**
The method of claim 23 where said selecting is performed in hardware on an integrated circuit including a microprocessor.	1:59-66 – "The second signal source is called a dummy traffic generator. The dummy traffic generator may be part of a repeater, which is a radio transceiver that receives signals on one frequency and retransmits these signals on another. A repeater is a communication unit generally designed to improve range in an RF communication system involving portable units, mobile units and fixed units." 1:67-2:6 – "The dummy traffic generator is capable of monitoring signals at the output of the repeater's receiver as well as any input that may be directed to the repeater from an associated control console. In the absence of signals from the receiver section of the repeater or from any console audio input, the dummy traffic generator transmits signals of its own in order to artificially increase the amount of traffic on the channel." 3:5-17 – "In normal operation, the output (106) of the signal source (101) is directed through the switch (103) to the transmitter (104). The dummy traffic generator (102) may also monitor the output of the first signal source (101) via a secondary output line (108). The dummy traffic generator (102) may, from time to time, switch its own output (107) through the switch (103) to the transmitter (104). This process artificially increases the amount of traffic appearing on the communication channel, thus making it difficult for an unauthorized user to obtain any information concerning the nature of the message traffic by noting any sudden increases in traffic volume." 3:30-40 – "The dummy traffic generator (204) is able to monitor the output of the receiver (202) through a secondary output line (211) and the console audio through a secondary audio line (212). When no receiver output or console audio is present, the dummy traffic generator (204) generates signals of its own from time to time. These signals are coupled from the dummy traffic generator output (209) through the switch (205) and on to the transmitter (206). Control of the switch (205) is achieved by the dummy traffic generator through